SOC IMS: SOC-20110808-224205

Last Updated: 10/25/2012 10:16 PM

SOC Incident Management System

IMS User Contact:	(b) (6), (b)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:		**Contact First Name:**	
Contact Role:		**Contact Office Phone:**	
Contact E-mail:		**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SOC-20110808-224205	**Categorization:**	Incident
Date Record Created (UTC):	8/8/2011 6:53 PM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	Possible Compromised Account		
Brief Description:	Email from (b) (6), (b) reporting possible compromised account. URL: (b) (2), (b) (7)(E)		
Current Status:	Resolved	**Assigned To:**	SOC Tier-2
Current Priority:	Medium	**Also Notify:**	CTAP
CUI:	Maybe SBU Only	**Notify on Save:**	No

CUI Categories:	
Ok To Close:	No

US CERT Reporting

Risk Rating:			
Information Impact:		**Functional Impact:**	
Recoverability:		**Attack Vectors:**	
Critical Service or System:		**Classified Incident:**	
Major Incident:		**High Value Assets (HVA):**	
Reportable to Congress:			
Observed Activity:		**Number of Records Impacted:**	
Location of Observed Activity:		**Number of Systems Impacted:**	
Actor Characterization:		**Number of Users Impacted:**	
Action Taken to Recover:		**Number of Files Impacted:**	

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old:		**Informational Impacts old:**	
		Recoverability Impact old:	

Sensitive But Unclassified

Reason SBU is suspected to be involved:		**How SBU was disclosed:**	
SBU Media Format:		**SBU Media Format Medium:**	
Date & Time Incident Occurred:		**Date & Time of Discovery of SBU Loss:**	

Scope of SBU Exposure:		**SBU Data Elements Exposed:**	
Original Information Owner:		**Number of Individuals without the appropriate "Need to Know" for Information Associated with this Exposure:**	
Protection of SBU Data Elements:		**SBU Trade Secrets:**	
Law Enforcement or IG Notified about SBU:		**Time to Report:**	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
No Records Found						

Related Incidents

Select Relationship:		**Relationship Description:**	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Incident Details

Time Incident Started:		**Time Incident Started (UTC):**	
Time Incident Detected:		**Time Incident Detected (UTC):**	
Center Affected by Incident:	Other	**Overall Impact (reference):**	Low

US-CERT Category:	CAT 1 - Unauthorized Access	**Incident Subcategory:**	
US-CERT Tracking Number:	INC000000167154	**ESD Ticket #:**	
Resolution Status:	False Positive	**Malware Family:**	
		Highest level of access gained:	
Primary Method used to Identify Incident:	NASA-CERT Security Operations Center (SOC)		
SOC Detection Method:			
Primary Attack Category:			
Primary Vulnerability Type:		**Lost or Stolen NASA Equipment:**	

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
No Records Found			

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:		**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
No Records Found		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment
No Records Found		

IOC Detection

Name	Type	Comment
No Records Found		

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:
(b) (7)(E) ."
See the help for the individual fields for more information about what the various values mean and their context.

Root Cause Sources:		**Root Cause Categories:**	
Root Cause Methods:		**Root Cause Causes:**	
Root Cause Factors:		**Root Cause Objectives:**	

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact
No Records Found						

Impact of Incident

NASA Programs, Projects, and/or Operations:		**People:**	

Data (at Rest or Transmission):		**System:**	
Cost:		**Sophistication / Nature of Attack:**	
Number of systems affected by this incident:		**Number of NASA Centers/ Facilities affected by this incident:**	
Number of accounts affected by this incident:		**Critical Infrastructure Impacted:**	
Other Impacts:			
Overall Impact:	Low -- Incident Considered Low if none of the below Categories are rated Moderate or High		

Containment Actions

Incident Containment System Action:	
Incident Containment Network Action:	

Recovery Actions

Incident Recovery System Action:	
Incident Recovery User Action:	

Recommendations

Root Cause:	
Lessons Learned:	

Costs

Center (Hours):	1.00	**Center (Dollars):**	100.00
NASA SOC (Hours):		**NASA SOC (Dollars):**	
NASA NOC (Hours):		**NASA NOC (Dollars):**	

Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	1	**Total Cost (Dollars):**	100
Description of Costs:			
System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record Opened (UTC):	8/8/2011 6:53 PM	**Date Record Confirmed (UTC):**	8/17/2011 11:24 PM
Date Record Contained (UTC):	8/17/2011 10:57 PM	**Date Record Resolved (UTC):**	8/17/2011 10:57 PM
Date Record Closed (UTC):			
Time in Open:	9.17		
Time in Confirmed:		**Time to Confirm:**	9.00
Time in Contained:		**Time to Contain:**	9.17
Time in Resolved:		**Time to Resolve:**	9.17
Time in Closed:		**Time to Close:**	
Number of Days to Resolve:	9.169		

Journal Entries

Entry	Entry Date	IMS User
No evidence found.	8/17/2011 10:55 PM	
(b) (7)(E) can't resolve IP. QR mine from "07/15/2011" to "08/02/2011" o (b) (7)(E) Attached as (b) (7)(E)	8/8/2011 9:42 PM	
Sent an email to (b) (6) asking for a Q Radar mine. This was a response to (b) (6) email.	8/8/2011 7:07 PM	

(SOC analyst),

When you get in, can you do a Q Radar mine to see if there have been any hits to any NASA server from (b) (7)(E) over the last week or so? My Q Radar account is still inaccessible (need a password reset).
I checked splunk and didn't see anything. Also, splunk isn't displaying anything for GSFC at the moment as it's listed as 'down'.

It's quite likely there's nothing from (b) (7)(E) that's just where a potential proof of SQL injection screenshot was posted.

The screenshot has been attached to ticket SOC-20110808-224205.

Attached the image that was posted on (b) (7)(E)	8/8/2011 7:01 PM	
Also on the one (b) (6) were reporting (that NIH sent us earlier too): The hash itself appears to have been reported/requested for cracking on Jully 22 by user "666": (b) (7)(E) 666 Joined: 08 Feb 2011 Posts: 72 (b) (7)(E) Posted: Fri Jul 22, 2011 11:17 am Post subject: (b) (7)(E) thnx Admin (b) (7)(E) -- IT Security Specialist NASA Office of the CIO Cyber Threat Analysis Program (CTAP) On 8/8/11 1:18 PM, wrote: > > > > Also saw this one: > > > > (b) (7)(E) > > > > > > Perhaps the SOC can open a separate ticket to look into this one. I am	8/8/2011 6:52 PM	

not
> > sure if the site is considered hostile or not. I've attached the image that
> > shows the issue to this e-mail. Can't tell the site or users though..
> >
> >(b)
> >
> >
> >
> > On 8/8/11 1:11 PM, (HQ-WIM51)"
> > wrote:
> >
>> FYI, from (b) (7)(E)
>>
>> ================
>>
>> Nasa Vulnerable to a public SQLi Exploit - Embarassing much?
>>
>> Admin Username (b)
>> Email: (b) (6), (b) (7)(C)
>> Hashed Password (b) (7)(E)
>> (b) (7)(E)
>>
>> Admin Username: (b) (6),
>> Email (b) (6), (b) (7)(C)
>> Hashed Password: (b) (7)(E)
(b) (7)(E)
>>
>> - If shit like this is vulnerable to public exploits, imagine whats
>> vulnerable
>> to private 0days :) -
>>
>> [+] TriCk - TeaMp0isoN
>> [+] Shoutouts: iN^SaNe - Hex00010 - MLT
>>
>> Twitter:
>> @TeaMp0isoN_
>>
>> **NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the
>> interwebs soon **
>>
>> =============
>>
>> SOC folks, can you check into this to try to determine what server might have
>> been affected, and let me know?
>>
>> Thanks,
>>
>>
>>
>> Special Agent
>> NASA OIG Computer Crimes Division
>> (b) (7)(C), (b) (6)
>> +1
>> PGP Key (b) (6), (b)
>>
>> ! WARNING ! This email including any attachments is intended only for

Attachment(s)

Name	Size	Type	Upload Date	Downloads
224205.csv	20483	.csv	8/8/2011 9:44 PM	1
nasa.png	85727	.png	8/8/2011 7:00 PM	1

History Log

View History Log